ホームページ公開文書

制定 2010年6月25日

画像診断ワークステーションのウイルス対策ソフトに関するガイドライン

Guideline for the anti-virus software in the image diagnosis workstations

－ 技術資料No． JESRA TR-0035^{-2010} －

（社）日本画像医療システム工業会

目次

序文

厚生労働省から発行されている「医療情報システムの安全管理に関するガイドライン」（参考文献(1)）では，医療情報を扱うシステムの基本的な安全管理について，不正ソフトウェア対策としては，ウイルス対策ソフトの導入が最も効果的で，そのためには，パターンファイルを常に最新のものに更新することが必須であるという趣旨の記載がある（参考文献(1)P40 6.5 (4)不正ソフトウェア対策）。

事実，情報化社会への進展に伴い，医療情報システムもコンピュータウイルスに代表される外部からの攻撃に対してセキュリティ対策（ウイルス対策ソフト，OS セキュリティ・パッチ，ユーザ管理，ファイアウォール等）が必要となっており，その中でも最も効果的であるウイルス対策ソフトの必要性が高まっている。特に汎用の技術を利用し，ネットワークシステム等の様々な環境で使用される画像診断ワークステーション（汎用画像診断装置ワークステーション等）は，コンピュータウイルスの攻撃を受けやすく，ウイルス対策ソフトは必須ツールとなってきている。そのため，画像診断ワークステーションにインストールされるソフトの中でもウイルス対策ソフトの運用方法の検討の必要性・緊急性は高いと言える。

しかしながら，医療機器である画像診断ワークステーションへのウイルス対策ソフトの適用については，当工業会でも会員企業各社で，まちまちの対応を取っており，自社の対応方法が適切かよくわからない，という意見がある。例えば，検索エンジン・パターンファイルの更新，バリデーション等について各社対応に苦慮しているという現状である。とはいえ，ネットワークシステムに接続されるため，医療機器だからといって特別扱いすることは現実にそぐわない。また，「医療情報システムの安全管理に関するガイドライン」でも具体的なウイルス対策ソフトの画像診断ワークステーションへの導入方法や更新に関する手順については記載がされていない。

以上の状況を鑑み，画像診断ワークステーションへのウイルス対策ソフトの適用についてガイドラインの作成を行った。本ガイドラインをもとにして，画像診断ワークステーションのみならず，その他の汎用 PC を使った機器のウイルス対策ソフトの導入にも参考としていただけると良いと考える。

1. 適用範囲と目的

1.1 適用範囲

本ガイドラインは，画像診断ワークステーションに市場にてインストールされるウイルス対策ソフトについて適用する。

1.2 目的

本ガイドラインは，画像診断ワークステーションにインストールされるウイルス対策ソフトについて，必要な運用方法やサービスを明確にして，医療機器としての画像診断ワークステーションの安全性，有効性を確保するものである。また，本ガイドラインは，ウイルス対策ソフトを必須とするものではない。例えば，スタンドアロンで使用される場合等は，それ以外の運用により対応することも十分可能と考えられる場合もあるため，医療機関の判断で必要な対策を講じればよいと考えられる。

2. 用語

本ガイドラインでは，便宜上使用する用語を以下の通り定義して使用することとする。

ウイルス対策ソフト:

コンピュータウイルス，ワーム等と呼ばれる不正ソフトウェアをコンピュータから見つけ出し，駆除する事を主な機能とするソフトウェア。アンチウイルスソフトウェアとも呼ぶ。

画像診断ワークステーション:

一般的名称の汎用画像診断装置ワークステーション，核医学装置ワークステーション，X 線画像装置ワークステーション，MR 装置ワークステーション，超音波装置ワークステーションを指す。

医療機関:

画像診断ワークステーションの使用者のことで，病院や診療所等を指す。

ウイルス対策ソフト業者:

ウイルス対策ソフトを製造する業者のこと。ウイルス対策ソフトメーカー。

3. ウイルス対策ソフトの概要

3.1 ウイルス対策ソフトの機能

ウイルス対策ソフトには，様々な機能が存在し，多くの製品が販売されている。一般的には，不正ソフトウェア対策機能，スパイウェア対策機能，不正アクセス防止機能等の機能を持つ製品があり，スタンドアロン型（個人向け）やネットワーク環境で利用するサーバ／クライアント型（企業向け）が利用されている。

a) 不正ソフトウェア対策機能

コンピュータウイルスやワーム等の不正ソフトウェアの検出，復旧，削除，隔離等を行う機能。

b) スパイウェア対策機能

スパイ活動を行うスパイウェアの侵入監視，検索／駆除，情報流出防止等を行う機能。

c) 不正アクセス防止機能

ファイアウォール機能による不正アクセス防止／侵入検知を行う機能。

3.2 ウイルス対策ソフトの構成

ウイルス対策ソフトは，ウイルスを検索するプログラム（検索エンジン）と，ウイルスを検出するためにウイルスの特徴やパターンを定義したデータファイル（パターンファイル，定義ファイルともいう）で構成されており，新たに発見されたウイルスに対応するために頻繁に更新されている。
最近は，これら検索エンジンとパターンファイルは，インターネットから自動的にダウンロードして，リアルタイムに更新するものが主流となっている。

3.3 ウイルス対策ソフトの稼動環境

3.3.1 システム構成

a） スタンドアロン型

個人利用や数台程度の小規模なネットワーク環境で利用され，ウイルス対策ソフト単体で構成される。

b） サーバ／クライアント型

中規模以上のネットワーク環境で利用され，管理サーバとウイルス対策ソフトを導入したクライアント機器（画像診断ワークステーション等）で構成される。

【管理サーバとは】

ウイルス対策ソフトの管理サーバとは，ウイルス対策ソフトの検索エンジン／パターンファイル等を一元管理するための専用サーバソフトで構成され，クライアント機器のウイルス感染の有無やパターンファイルの更新状況等を管理するために利用される。

3.3.2 ネットワーク

医療機関のネットワーク環境は，セキュリティポリシーの違いやネットワーク管理者の有無により，様々な形態が存在する。以下にその例を示すが，本ネットワーク環境は後述のパターンファイルの更新方法等と密接に関係するため，ウイルス対策ソフトの導入を検討する際には，インターネットの利用可否を含めて事前に十分な確認，検討を行う必要がある。

【医療機関内LANと外部ネットワーク（インターネット）との接続形態】

a） 物理的に隔離

外部ネットワークと接続していないローカルなネットワーク環境

b） プロキシ・ファイアウォール経由で接続

プロキシサーバ（代理サーバ）やファイアウォールを利用して外部ネットワークが利用可能なネットワーク環境

c） ルータ等を介して接続

ルータ機器の直下に接続され，外部ネットワークが利用可能なネットワーク環境

3.4 ウイルス対策ソフトの保守

ウイルス対策ソフトのパターンファイルの更新方法は，主にインターネットを利用して更新を行う「オンライン運用」，ウイルス対策ソフト業者のサイトから取得した更新ファイルをメディア等でクライアント機器に取り込む「オフライン運用」，ウイルス対策ソフトの管理サーバを用いた「管理サーバ運用」などがある。

3.4.1 オンライン運用

インターネットが利用できる場合には，ウイルス対策ソフト業者のサイトから更新ファイルを直接取得して更新する方法（オンライン方式）が利用可能である。

3.4.2 オフライン運用

インターネットを直接利用できない場合には，インターネットが利用可能なPCを使って，ウイルス対策ソフト業者のサイトから取得した更新ファイルをメディア等でクライアント機器に取り込むことが可能である（オフライン方式）。

3.4.3 管理サーバ運用

ウイルス対策ソフトの管理サーバ（以下，管理サーバ）を用いることで，ウイルス対策ソフトを導入したクライアント機器に更新ファイル（パターンファイル／検索エンジン）の配信・管理が可能である。また，クライアント機器側でインターネットが利用できない環境でもパターンファイルを更新することが可能となり，同時にクライアント機器のウイルス感染の検出も可能なため，効率的なウイルス対策の管理方法として広く利用されている。

【管理サーバの更新ファイルの更新方法】

インターネットから直接更新ファイルを取得する方法（オンライン方式）とインターネットが利用可能なPCを使って，ウイルス対策ソフト業者のサイトから取得した更新ファイルをメディア等で管理サーバに取り込む方法（オフライン方式）がある。

3.5 ウイルス検出機能

ウイルス検出機能には，「リアルタイムスキャン」と「フルスキャン」の2種類があり，各機能の特性を理解し，医療機器への影響を考慮した適切な設定が必要となる。

3.5.1 リアルタイムスキャン

リアルタイムスキャンとは，外部からのウイルス感染を常時監視する機能であり，コンピュータのメモリやローカルドライブ上のファイルの作成，コピー，実行，名前変更等の操作が行われたときに，

ウイルススキャンが行われ，ウイルスを検出した場合には，ウイルスの駆除や隔離を行う。

3.5.2 フルスキャン

フルスキャンとは，スケジュールあるいは必要に応じて適宜実行されるウイルススキャンである。リアルタイムスキャンで発見できなかった新種のウイルスのチェックや，設定によりリアルタイムでは監視していないファイル，フォルダなどのチェックを行うことができるため，定期的に行うことが推奨されている。

3.6 リスクの低減手段

ウイルス対策ソフトの導入に伴い，画像診断ワークステーションのパフォーマンス低下やパターンファイル不具合の影響を受ける可能性がある。ウイルス対策ソフトの設定や運用を工夫することでこれらのリスクを低減することが出来る。以下にその例を示す。

3.6.1 リアルタイムスキャンの除外設定

画像診断ワークステーションで画像データを扱う場合には，データが保存されるフォルダ等をリアルタイムスキャンの対象から除外する設定を行うことで，パフォーマンス低下を大幅に抑制することができる。但し，これら特定のフォルダを除外することで，ウイルス感染のリスクが生じる為，定期的なフルスキャン機能と併用した運用が必要である。

3.6.2 定期スキャン

リアルタイムスキャンのフォルダ除外を行う場合には，除外フォルダを含めた全てのファイルに対して定期的にフルスキャンを実行し，ウイルス感染が無いことを確認する運用が好ましい。この定期スキャンでは，過去のリアルタイムスキャンでは発見できなかったウイルスが潜伏しているような場合でも発見できる可能性があり，実施することが推奨される。

3.6.3 更新タイミングの制御

ウイルス対策ソフトの有効性を高めるためにパターンファイルの更新は重要であるが，パターンファイル自体の不具合により動作異常を引き起こす可能性もある。パターンファイルの更新タイミングを遅らせることや，評価済みのパターンファイルを導入することなどで，不具合の影響を回避できる可能性がある。ただし，更新が遅れることによる感染リスクは増すため，総合的なバランスを踏まえた制御が必要である。

4. ウイルス対策ソフトのガイドライン

4.1 使用するウイルス対策ソフトの位置づけ

ウイルス対策ソフトそのものは，医療上の効能・効果をもつものではないが，画像診断ワークステーションと市場で組み合わされて使用されるものである。よって，ウイルス対策ソフトのために画像

診断ワークステーションの有効性，安全性が損なわれないよう，以降で示す基準を設け，対応する必要がある。また，必要に応じ，製造販売業者が扱うウイルス対策ソフト（推奨ウイルス対策ソフト）に関する説明を画像診断ワークステーションの取扱説明書等に記載する。

4.2 推奨ウイルス対策ソフトの選定

製造販売業者は，4.3　ウイルス対策ソフトのバリデーションに示す作業を行い，問題のないことが確認されているソフトウェアを推奨ウイルス対策ソフトとして選定しておく必要がある。

4.3 ウイルス対策ソフトのバリデーション

製造販売業者は，事前に画像診断ワークステーションにウイルス対策ソフトをインストールして安全性，有効性の評価を行い，ウイルス対策ソフトも正常に稼動することを確認することが必要である。バリデーションは，初期導入前と更新ファイルの評価に分類され，以下の観点に基づいて行う。

4.3.1 初期導入前のバリデーション確認事項

a) ウイルス対策ソフトをインストール手順書（下記参照）に従ってインストールし，問題なくインストールできること。
b) ウイルス対策ソフトインストール後に再起動し，画像診断ワークステーションが稼動すること。（起動，終了）
c) ウイルス対策ソフトが正常に稼動すること。（例えば，マニュアル通りの動作が出来る等）
d) ウイルス対策ソフトを稼動させた状態で，画像診断ワークステーションが意図した通りに稼動すること。例えば，ウイルス対策ソフトの設定（スキャン対象フォルダやスキャンを行う時間帯等）で画像診断ワークステーションのパフォーマンスが運用に支障がでるほど低下しないこと。

4.3.2 更新に関する定期的なバリデーション確認事項

更新に関する定期的なバリデーションの評価間隔は，製造販売業者の評価能力や更新ファイルの提供手段等の事情に合わせて決定する。
a) 検索エンジン及びパターンファイルの更新を行い最新の状態にする。
b) ウイルス対策ソフトを稼動させた状態で，画像診断ワークステーションが意図した通りに稼動すること。
c) ウイルス対策ソフトが正常に稼動すること。（例えば，マニュアル通りの動作が出来る等）

4.4 ウイルス対策ソフトのインストールとインストール手順書

実施者：販売業者又は販売業者の委託する修理業者（以降，販売業者（修理業者）と記述）
手順：製造販売業者が作成するインストール手順書にもとづき行う。

ウイルス対策ソフトのインストールは，一般的に複雑な手順を含む場合が少なくない。また，画像診断ワークステーション環境によって，インストール方法が異なっていたりする場合があるので，イ

ンストールの失敗を防ぐためにも販売業者（修理業者）が行う必要がある。インストール作業は，以下の観点に沿ってインストール手順書を作成し，その手順書に従ってインストールを行われなければならない。

【インストール手順の確認事項】
a) インストールに関する記録（対象画像診断ワークステーションの情報，インストールする対象の環境の情報，作業者情報等）を作成，保管すること。
b) インストール中に行うウイルス対策ソフトの設定が上記の「ウイルス対策ソフトのバリデーション」によって決められている場合は，これを設定作業に加えること。
c) インストールが問題なく終了したことを確認すること。
d) インストールが複数の画像診断ワークステーションに行われる場合は，すべての画像診断ワークステーションについてインストールが完了したこと確認すること。
e) インストールが失敗した場合は，画像診断ワークステーションがその後も問題なく稼動することを確認すること。
f) インストール手順書は，インストール作業者が画像診断ワークステーションのある医療機関で実施することも想定して作成すること。このためにインストール作業が，医療機関の医療情報システムの運用の妨げにならないようにすること。

4.5 ウイルス対策ソフトの保守

コンピュータウイルスは，日々発生しており，これに対応するためにウイルス対策ソフトのパターンファイルも日々更新されているのが実態である。パターンファイルの更新が遅れたためにコンピュータウイルスに感染した，という事例も報告されているため，画像診断ワークステーションにインストールするウイルス対策ソフトのパターンファイルの更新も常に最新の状態にしておくことが必要である。（参考文献(2),(3),(4)）

しかしながら，実際のパターンファイルの更新サイクルは短いため，例えば毎日の更新のたびに製造販売業者がバリデーションして医療機関に配布することは現実的でない。現実的な対応としては，製造販売業者が機器保守作業の一環として定期的なバリデーションを実施し，更新ファイル（検索エンジン及びパターンファイル）を医療機関に提供することである。（4.3 ウイルス対策ソフトのバリデーション参照）

そこで医療機関のウイルス対策ソフト以外のセキュリティ対策が重要となる。ウイルス感染の原因となるUSBメモリの使用制限やファイアウォール等を導入するなどして医療機関のセキュリティ対策が十分であるならば，製造販売業者が定期的にバリデーションした検索エンジン及びパターンファイルを医療機関に配布すればよいと考えられる。

一方，医療機関のセキュリティポリシーとして，短期間で更新する必要がある場合には，医療機関の日々の始業前点検と製造販売業者の定期的なバリデーションを組み合わせて実施する。画像診断ワークステーション使用中に新たな更新が発生しないように，始業前点検の前に更新される設

定が望ましい。始業前点検方法については，製造販売業者が，医療機関に情報を提供し，点検方法を決める際の参考とする。始業前点検には，使用者による日常の保守点検として取扱説明書等に以下の観点を含めるとよい。

a) OS の起動確認。

b) 画像診断ワークステーションのソフトウェアの起動確認。

c) 動作速度が通常と比較して著しく低下してないかの確認。

なお，更新方法は，ネットワーク経由で配信される更新ファイルによるものが多いと考えられるが，正常に更新できる仕組みであることは，インストール時等に販売業者（修理業者）が医療機関とともに確認する。また，更新ファイルには，検索エンジンとパターンファイルの両方の更新情報が含まれていることがあり，両者を分離して行うことは難しく，検索エンジンの更新もパターンファイルの更新と同様の扱いとする。検索エンジンがパターンファイルと分離できる場合は，更新による不具合とウイルス感染のリスクを比較して，バリデーション内容と更新時期を決めることが望ましい。例えば，ウイルス対策ソフト業者から，事前に更新情報を入手できる場合は，製造販売業者が 4.3.2 更新に関する定期的なバリデーション確認事項を行うなどがある。

以上のように，ウイルス対策ソフトの保守は，医療機関のセキュリティ対策で対応が異なるため，以下の点を考慮して，事前にどのような対応を取るかを十分医療機関と話し合い，保守方針を取り決める必要がある。

4.5.1 製造販売業者の保守方針

販売業者（修理業者）は，製造販売業者のバリデーションの方法に基づいたウイルス対策ソフトの保守方針を，医療機関に説明する。

a) 更新ファイルの更新間隔（例. 数ヶ月間隔，定期点検時など）

b) 更新ファイルの更新方法（例. ネットワーク経由での配信，メディアで提供，定期点検時など）

4.5.2 医療機関側での保守方針の決定

医療機関では，医療機関のセキュリティポリシーと製造販売業者の保守方針に基づいて保守方針を決定する。

a) 製造販売業者の提案内容で行う場合

製造販売業者の保守方針が医療機関のセキュリティポリシーに沿う場合には，製造販売業者の提案内容に基づいて保守を行う。

b) 医療機関のセキュリティポリシーで行う場合

製造販売業者の保守方針が医療機関のセキュリティポリシーに沿わない（十分でない）場合には，医療機関側で更新ファイルの更新間隔や更新方法を決定し保守を行う。この場合，前述のように医療機関側の日々の始業前点検と製造販売業者の定期的なバリデーションを組み合わせて実

施する等の対応が必要である。

4.6 ウイルス感染時の対応方法

ウイルス対策ソフトがインストールされていれば，基本的にウイルスの感染は防げるはずだが，パターンファイルの更新が頻繁でなかったり，ウイルス対策ソフトのシステム設定が十分でなかった場合等に感染する恐れがある。そのような場合には，インストールされたウイルス対策ソフトを使用して，復旧することが可能と考えられるが，以下の手順を事前に取り決めておく必要がある。

【ウイルス感染時の対応手順】

a) さらに感染が広がらないための手順，感染が報告された画像診断ワークステーションをネットワークから切断するためにネットワークケーブルをはずす等。

b) 使用するウイルス対策ソフトの検索エンジン，パターンファイルが最新であることを確認する手順。最新でなかった場合に更新する手順。

c) 確認したウイルス対策ソフトを用いて画像診断ワークステーションをスキャンする手順。

d) 感染が報告された画像診断ワークステーション以外のネットワークに接続された感染した画像診断ワークステーションを特定しスキャンする手順。

e) ウイルスが駆除されたことを確認した後に画像診断ワークステーションのシステムを復旧させる手順。

ウイルス感染により故障が発生した場合の復旧作業は修理行為であるため，修理業者が行うが，状況に応じて画像診断ワークステーションを所有する医療機関と作業分担を取り決めればよいと考えられる。

4.7 医療機関との確認事項

本章ではウイルス対策ソフトを導入するにあたり，医療機関と販売業者（修理業者）間で確認しておく主な事項を記載する。医療機関のセキュリティポリシーや販売業者（修理業者）の事情等を考慮して，確認事項を決める必要がある。参考として，本ガイドラインを踏まえた運用事例を表 1 に示す。

a) 導入するウイルス対策ソフト

販売業者（修理業者）は，製造販売業者が選定した推奨ウイルス対策ソフトを医療機関に提案する。取り扱うソフトが推奨ウイルス対策ソフトであることを確認する。

b) ウイルス対策ソフトの運用

リアルタイムスキャン・フルスキャンの実施時間帯，スキャン対象フォルダについて確認を行う。3.5 ウイルス検出機能，3.6 リスクの低減手段，4.3 ウイルス対策ソフトのバリデーションの項参

照。

c）ウイルス対策ソフトの保守方法

更新方法について以下に示す事項の確認を行う。4.5　ウイルス対策ソフトの保守の項参照。

1）更新の手段

3.4　ウイルス対策ソフトの保守の項参照。

2）更新タイミング

更新タイミングが遅れることや定期的な更新となること，更新しないこともあること等。3.6.3　更新タイミンングの制御，4.5　ウイルス対策ソフトの保守の項参照。

d）ウイルス感染時の対応方法と役割分担

4.6　ウイルス感染時の対応方法の項参照。

表1　ウイルス対策ソフトの運用事例

<table>
<tr><th colspan="2">事項</th><th>運用事例</th></tr>
<tr><td colspan="2">推奨ウイルス対策ソフト</td><td>製造販売業者が選定する。</td></tr>
<tr><td colspan="2">ウイルス対策ソフトのバリデーション（初期導入前）</td><td>製造販売業者が確認する。</td></tr>
<tr><td colspan="2">ウイルス対策ソフトのインストール</td><td>販売業者又は販売業者の委託する修理業者が行う。</td></tr>
<tr><td rowspan="2">検索エンジン及びパターンファイルの更新</td><td>バリデーション</td><td>①製造販売業者の定期的なバリデーションのみ
又は
②医療機関が行う日々の始業前点検と製造販売業者の定期的なバリデーション。（製造販売業者がバリデーションをする前に短期間で更新する場合）製造販売業者は，始業前点検方法の情報を医療機関に提供する。
（①，②は医療機関のセキュリティポリシー等により選択する。）</td></tr>
<tr><td>更新作業</td><td>医療機関が行う。</td></tr>
<tr><td colspan="2">ウイルス感染による故障発生時の対応</td><td>ウイルス感染により故障した場合の復旧作業は修理行為であるため修理業者が行う。</td></tr>
<tr><td colspan="2">取扱説明書等</td><td>・推奨ウイルス対策ソフトの説明を記載する。
・始業前点検の内容を記載する。</td></tr>
</table>

5．その他のウイルス対策方法

本ガイドラインは，不正ソフトウェア対策として最も効果的である「ウイルス対策ソフトの導入」について取り上げているが，この対策のみで全ての不正ソフトウェアが検出できるわけではないため，

画像診断ワークステーション側の脆弱性を可能な限り小さくしておくことの重要性を製造販売業者も十分に理解し，OS等の脆弱性対策（セキュリティ・パッチの逐次更新）も併せて対応することで，総合的な不正ソフトウェア対策を医療機関に提供することができる。

6. 参考文献

(1) 医療情報システムの安全管理に関するガイドライン，第 4.1 版，厚生労働省，平成 22 年 2 月
(2) Defending Medical Information Systems Against Malicious Software, Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC), December 2003
(3) Patching Off-the-Shelf Software Used in Medical Information Systems , Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC), November 2004
(4) Guidance for Industry, Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, CDRH FDA U.S. Department of Health and Human Services, January 2005

解説

1. 制定の趣旨

ネットワーク接続され、汎用の技術を利用した画像診断ワークステーション(汎用画像診断装置ワークステーション等)のコンピュータウイルス対策としては、ウイルス対策ソフトの導入が最も効果的であるといわれている。しかしながら、医療機器である画像診断ワークステーションへのウイルス対策ソフトの適用については、品質、有効性及び安全性の観点でどのように対応すべきかの統一見解が整備されていなかった。このことより、画像診断ワークステーションへのウイルス対策ソフトの適用についてガイドラインの作成が望まれていた。本ガイドラインはこの要望に応えるべく発行するものである。

2. 制定の経緯

この趣旨を実現すべく JIRA はソフトウェア委員会にワーキンググループ(ソフトウェア新WG1)を結成し，アンケートを実施し、検討を進めてきた。そして、厚生労働省の担当部署の御意見をいただき発行することとなった。

3. 審議過程での特記事項

3.1 ウイルス対策ソフトの位置づけ

ウイルス対策ソフトの位置づけについては、医療上の効能・効果をもたないが、画像診断ワークステーションと組み合わせて使用されるものであるため、その説明を取扱説明書等に記載することが妥当となった。

3.2 適用範囲

ウイルス対策ソフトによる不具合は基本的には少ないが、不具合があった場合も遅くなる程度で影響の少ない画像診断ワークステーションに市場にてインストールされるウイルス対策ソフトを適用範囲とした。また、その他の汎用 PC を使った機器のウイルス対策ソフトの導入についても参考にできるとした。しかしながら、撮影装置で不具合があった場合は撮影ができなくなる等の影響が大きく、慎重な対応が望まれるため対象外とした。

3.3 ウイルス対策ソフトの保守

ウイルス対策のパターンファイルは日々更新されているため、会員企業では更新のたびにバリデーションすることは現実的でないという意見が多数を占めた。しかしながら、医療機関のセキュリティポリシー等で、短いサイクルでの更新を要求される場合がある。

これに対応するために、本ガイドラインでは、更新のバリデーションについては製造販売業者の定期的なバリデーションのみで行う場合と医療機関の日々の始業前点検と製造販売業者の定期的なバリデーションを組み合わせて行う場合にわけて記載した。

4. 原案作成及び審査

4.1 原案作成：

法規・安全部会

部会長	古川 浩	東芝メディカルシステムズ(株)

ソフトウェア委員会

委員長	軸丸 幸彦	コニカミノルタエムジー(株)
副委員長	鴛田 栄二	富士フイルム(株)
副委員長	中島 京子	GE ヘルスケア・ジャパン(株)

ソフトウェア新 WG1

主査	小澤 啓一郎	富士フイルム(株)
副主査	佐藤 勝則	東芝メディカルシステムズ(株)
副主査	中島 京子	GE ヘルスケア・ジャパン(株)
	葉賀 功	コニカミノルタエムジー(株)
	繁村 直	テラリコン・インコーポレイテッド
	青木 弘幸	(株)フォトロンメディカルイメージング
	渡辺 裕章	コニカミノルタエムジー(株)
	小野 英二	(株)日立メディコ
	岡庭 貴志	(株)イメージワン
	辻井 修	キヤノン(株)
	和田 正人	(株)モリタ製作所
	大野 英	(株)グッドマンヘルスケア IT ソリューションズ
	伊藤 伸昭	パナソニックメディカルソリューションズ(株)

JESRA　TR-0035:2010
2010 年 6 月発行

発行 （社）日本画像医療システム工業会
〒113-0033 東京都文京区本郷 3-22-5
住友不動産本郷ビル9階
TEL 03-3816-3450
FAX 03-3818-8920